That which is claimed:

1. A network security system, comprising:

a static policy data store;

a dynamic policy data store;

an authorization enforcement facility (AEF) in communication with said static policy data store and said dynamic policy data store and operable to perform a risk-aware analysis of a connection.

2. The network security system of claim 1, wherein said static policy data store comprises at least one of a constraint, a role, a node-role assignment, a threshold value, a node value, a service value, and an action value.

3. The network security system of claim 2, wherein said threshold value is inversely proportional to said node value.

4. The network security system of claim 2, wherein said threshold value is inversely proportional to said node value.

5. The network security system of claim 1, wherein said dynamic policy data store comprises a threat level table.

6. The network security system of claim 1, wherein said AEF is further operable to generate a response to said connection.

7. The network security system of claim 6, wherein said response comprises at least one of blocking the source of said connection from connecting to an intended destination, altering said intended destination of said connection, and auditing said connection.

8. The network security system of claim 1, wherein said AEF is further operable to generate a countermeasure.

9. The network security system of claim 8, wherein said wherein said countermeasure comprises an active countermeasure or a passive countermeasure.

10. The network security system of claim 1, wherein said AEF comprises a router, a gateway, a hardware appliance, or a web server.

11. The network security system of claim 1, further comprising a firewall in communication with said AEF.

12. The network security system of claim 1, further comprising an intrusion detection system in communication with said AEF.

13. A method comprising:
receiving a static policy data attribute from a static policy data store;
receiving a connection request directed to a node;
receiving a dynamic policy data attribute from a dynamic policy data store;
determining whether said connection request is anomalous based at least in part on said static policy data attribute and at least in part on said dynamic policy data attribute.

14. The method of claim 13, further comprising responding to said connection request.

15. The method of claim 14, wherein responding comprises at least one of forwarding said connection request to said node; blocking the source of said connection from connecting to an intended destination, altering said intended destination of said connection, and auditing said connection.

16. The method of claim 13, further comprising updating said dynamic policy data attribute in said dynamic policy data store based on a result of said determining.

17. The method of claim 13, wherein said updating comprises increasing a threat level if the connection request is determined to be anomalous.